

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

Judge Robert S. Lasnik

March 1 20 18

By William M. McCool, Clerk  
Deputy

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,

NO. CR17-0290RSL

Plaintiff,

**SECOND SUPERSEDING  
INDICTMENT**

v.

MUHAMMAD FAHD and  
GHULAM JIWANI,

Defendants.

The Grand Jury charges that:

**INTRODUCTION**

At all times material to this Second Superseding Indictment:

1. AT&T Mobility LLC (hereinafter, AT&T), was a company with headquarters in Atlanta, Georgia, and offices throughout the United States, including a customer service call center in Bothell, Washington.

2. AT&T sold cellular telephones and offered monthly voice and data plans for use with the phones on the AT&T wireless network. AT&T phones and wireless services were sold through authorized AT&T dealers and retailers across the country.

3. New cellular phones, such as iPhones, cost hundreds of dollars, with many top-end models costing over \$500. To make phones more affordable, AT&T either subsidized the purchase cost of phones or provided an option to purchase phones under

1 an interest-free installment plan. To be eligible for either option, customers needed to  
 2 agree to enter into long-term service contracts that bound them to AT&T's wireless  
 3 network.

4 4. AT&T used proprietary locking software on AT&T phones that prevented  
 5 the phones from being used on any wireless network other than the AT&T network  
 6 unless and until the phones were "unlocked."

7 5. "Unlocking" a phone disabled the proprietary locking software and thereby  
 8 allowed the phone to be used on multiple carrier systems rather than exclusively with  
 9 AT&T.

10 6. The Wireless Customer Agreement between AT&T and each of its  
 11 customers provided that AT&T would unlock the customer's phone upon the satisfaction  
 12 of certain criteria, such as when the customer had satisfied the terms of his or her service  
 13 contract and/or installment plan.

14 7. Unlocked phones were a valuable commodity because they could be resold  
 15 and used on any other compatible network around the world. If an AT&T customer's  
 16 phone was unlocked with or without authorization, that customer could switch to another  
 17 carrier. If this happened, AT&T would be deprived of the remaining value of the  
 18 customer's service contract and, if applicable, remaining payments under the customer's  
 19 installment plan.

20 8. When phones were unlocked fraudulently without AT&T's authorization  
 21 and customers switched service to other carriers, the fraudulent transactions deprived  
 22 AT&T of the stream of payments that were due under the service contracts and  
 23 installment plans.

24 9. AT&T employees at AT&T's Mobility Customer Care call center in  
 25 Bothell, Washington, had access to AT&T's computer systems to assist AT&T customers  
 26 with service and billing issues. Among other things, AT&T employees at the call center  
 27 had the ability to submit unlock requests on behalf of eligible customers.

10. AT&T employees used a variety of internal computer programs at AT&T to process unlock requests. Access to the systems was limited to authenticated users connected to AT&T's internal and protected corporate network.

11. AT&T's unlocking systems permitted AT&T employees with proper authorization and network credentials to, in appropriate circumstances, send requests to unlock the phones of AT&T customers.

12. Malware was malicious computer code running on a computer that was not authorized by the owner/authorized user of that computer. Malware could be designed to do a variety of things, including logging every keystroke on a computer, stealing information or “user credentials” (passwords or usernames), and executing unauthorized commands without the consent of the authorized user.

**COUNT 1**  
**(Conspiracy to Commit Wire Fraud)**

13. The allegations contained in Paragraphs 1 through 12 of this Second Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

## I. THE OFFENSE

14. Beginning at a date unknown, but no later than April 2012, and continuing through in or about September 2017, at Bothell, within the Western District of Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM JIWANI, and others known and unknown to the Grand Jury, did knowingly and intentionally, agree and conspire to devise and execute and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals

1 and sounds as further described below, in violation of Title 18, United States Code,  
2 Section 1343.

3 **II. THE OBJECT OF THE CONSPIRACY**

4 15. The object of the conspiracy was to gain access to AT&T's protected  
5 internal computers without authorization, and in excess of authorization, by bribing  
6 AT&T employees to submit fraudulent and unauthorized cellphone unlocking requests  
7 through AT&T's internal protected computer network through, among other means, the  
8 installation of malware and unauthorized hardware on AT&T's internal network. The  
9 object further was to sell to members of the public the resulting ability fraudulently to  
10 unlock phones, so that the members of the public could stop using AT&T wireless  
11 services and thereby deprive AT&T of the stream of payments it was owed under the  
12 customers' service contracts and installment plans.

13 **III. MANNER AND MEANS OF THE CONSPIRACY**

14 **A. Overview of the Conspiracy**

15 16. It was part of the conspiracy that MUHAMMAD FAHD, GHULAM  
16 JIWANI and others known and unknown to the Grand Jury, gained unauthorized access  
17 to AT&T's internal protected computers through a variety of methods, including by  
18 bribing AT&T employees (hereinafter "insiders") at AT&T's call center in Bothell,  
19 Washington, to use their network credentials and exceed their authorized access to  
20 AT&T's computers to submit large numbers of fraudulent and unauthorized unlock  
21 requests on behalf of the conspiracy and to install malware and unauthorized hardware on  
22 AT&T's systems.

23 17. From in or about April 2012 to in or about April 2013, MUHAMMAD  
24 FAHD, and others known and unknown to the Grand Jury, transmitted instructions to the  
25 insiders via the wires in interstate and foreign commerce, including lists of cellular  
26 telephone international mobile equipment identity (IMEI) numbers for the insiders to  
27 submit for fraudulent and unauthorized unlocking.

1       18. From in or about April 2013 to in or about October 2013, MUHAMMAD  
2 FAHD, GHULAM JIWANI and others known and unknown to the Grand Jury, bribed  
3 insiders to plant malware on AT&T's internal protected computers for the purpose of  
4 gathering confidential and proprietary information on how AT&T's computer network  
5 and software applications functioned.

6       19. Using information gathered by this malware about AT&T's computer  
7 network and software applications, MUHAMMAD FAHD, and others known and  
8 unknown to the Grand Jury, created additional malware designed to interact with  
9 AT&T's internal protected computers and process fraudulent and unauthorized unlock  
10 requests submitted over the wires in interstate commerce from remote servers controlled  
11 by members of the conspiracy.

12       20. The malware MUHAMMAD FAHD, and others known and unknown to  
13 the Grand Jury, planted on AT&T's internal protected computers used network  
14 credentials that belonged to actual AT&T employees, including co-conspirators and  
15 others, to allow MUHAMMAD FAHD, and others known and unknown to the Grand  
16 Jury, to log into AT&T's internal protected computers under false pretenses and to  
17 process fraudulent and unauthorized unlock requests.

18       21. From in or about November 2014 to in or about September 2017,  
19 MUHAMMAD FAHD, GHULAM JIWANI and others known and unknown to the  
20 Grand Jury, bribed insiders to use their access to AT&T's physical work space to install  
21 unauthorized computer hardware devices, including wireless access points designed to  
22 provide the conspiracy with unauthorized access to AT&T's internal protected computers  
23 and facilitate the automated process of submitting fraudulent and unauthorized unlock  
24 requests on behalf of the conspiracy.

25       22. The unauthorized computer hardware devices, like the malware, used  
26 network credentials that belonged to actual AT&T employees, including co-conspirators  
27 and others, and allowed MUHAMMAD FAHD, and others known and unknown to the  
28

1 Grand Jury, to log into AT&T's internal protected computers under false pretenses and to  
 2 process fraudulent and unauthorized unlock requests.

3       23. During the course of the conspiracy, MUHAMMAD FAHD, GHULAM  
 4 JIWANI, and other co-conspirators who were not associated with AT&T, paid more than  
 5 \$1,000,000 in bribes to AT&T insiders who joined the conspiracy. MUHAMMAD  
 6 FAHD, GHULAM JIWANI, and other co-conspirators paid these bribes to induce the  
 7 AT&T insiders to unlock cellular phones without authorization, including by installing  
 8 malware and unauthorized hardware on AT&T's computer systems.

9       24. During the course of the conspiracy, the conspirators caused more than  
 10 2,000,000 cellular telephones fraudulently to be unlocked by AT&T through the AT&T  
 11 insiders' submission of fraudulent unlocking requests and through the conspirators' use  
 12 of malware and hardware installed on AT&T's systems by the AT&T insiders to conduct  
 13 unauthorized unlocks.

14 **B. Defendant MUHAMMAD FAHD's Participation in the Conspiracy**

15       25. It was part of the conspiracy that MUHAMMAD FAHD, doing business as  
 16 Endless Trading FZE (aka Endless Trading FZC), Endless Connections Inc., and  
 17 iDevelopment Co. recruited insiders at AT&T who were willing to take bribes to work on  
 18 behalf of the conspiracy.

19       26. MUHAMMAD FAHD contacted the insiders at AT&T via telephone,  
 20 Facebook, and other communication channels in interstate and foreign commerce and  
 21 offered to pay them to unlock cell phones. MUHAMMAD FAHD instructed the insiders  
 22 to obtain pre-paid cellular phones and anonymous online email accounts to communicate  
 23 with him.

24       27. MUHAMMAD FAHD also instructed the insiders to create shell  
 25 companies and open business banking accounts in the names of the shell companies to  
 26 receive payments for their work on behalf of the conspiracy.

1       28. MUHAMMAD FAHD obtained lists of IMEI numbers for cellular  
 2 telephones from co-conspirators, and others, who operated businesses that offered  
 3 unlocking services to customers for a fee.

4       29. Beginning in or about August 2012, MUHAMMAD FAHD and GHULAM  
 5 JIWANI sent lists of IMEI numbers for cellular telephones via the wires in interstate and  
 6 foreign commerce to the insiders with instructions to submit unauthorized unlock  
 7 requests for the IMEIs using their access to AT&T's protected internal computer  
 8 network.

9       30. Beginning in or about April 2013, MUHAMMAD FAHD sent malware to  
 10 the insiders via the wires in interstate and foreign commerce and instructed them to install  
 11 the malware on AT&T's computer network. The malware was designed to gather  
 12 confidential and proprietary information regarding the structure and functioning of  
 13 AT&T's internal protected computers and applications.

14       31. Using information collected by the malware, MUHAMMAD FAHD, and  
 15 others known and unknown to the Grand Jury, created additional malware designed to  
 16 facilitate the transmission of commands via the wires in interstate and foreign commerce  
 17 from a remote server to AT&T's protected internal computer network and to submit  
 18 unauthorized unlock requests.

19       32. MUHAMMAD FAHD sent the insiders multiple versions of the unlocking  
 20 malware to test and perfect the malware on behalf of the conspiracy. Once the malware  
 21 was perfected, MUHAMMAD FAHD instructed the insiders to plant the unlocking  
 22 malware on AT&T's internal protected computers and to run the unlocking malware  
 23 while they were at work. The unlocking malware used valid AT&T network credentials  
 24 that belonged to co-conspirators and others, without authorization, to interact with  
 25 AT&T's internal protected computer network and process automated unauthorized  
 26 unlock requests submitted from an external server.

27       33. In or about October 2013, AT&T discovered the unlocking malware and  
 28 identified several insiders who were operating the unlocking malware at MUHAMMAD

1 FAHD's direction. Those insiders subsequently left AT&T after being approached by  
 2 AT&T investigators.

3       34. As a result, beginning in or about November 2014, MUHAMMAD FAHD  
 4 recruited new insiders at AT&T willing to accept bribes to work on behalf of the  
 5 conspiracy.

6       35. MUHAMMAD FAHD and others known and unknown to the Grand Jury,  
 7 began programming hardware devices designed to facilitate unauthorized access to  
 8 AT&T's internal protected network for the purpose of processing unauthorized unlock  
 9 requests.

10      36. MUHAMMAD FAHD provided the hardware devices to co-conspirators  
 11 including current and former AT&T insiders who tested the devices. Upon perfecting the  
 12 operation of the devices, MUHAMMAD FAHD provided the devices to insiders who  
 13 plugged the devices into AT&T's internal protected network without authorization to  
 14 facilitate the unlocking of phones in furtherance of the conspiracy.

15      37. MUHAMMAD FAHD continued to pay insiders at AT&T to gain  
 16 unauthorized access to AT&T's internal protected computer network, and exceed their  
 17 authorized access to AT&T's protected internal computer network to plant malware,  
 18 install unauthorized hardware, and operate malware and unauthorized hardware on  
 19 AT&T's protected internal computer network on behalf of the conspiracy through in or  
 20 about September 2017.

21 **C. Defendant GHULAM JIWANI's Participation in the Conspiracy**

22      38. It was part of the conspiracy that GHULAM JIWANI received lists of  
 23 thousands of IMEIs from customers of the conspiracy and from co-conspirators that those  
 24 customers wanted to have unlocked. The customers and co-conspirators who provided  
 25 GHULAM JIWANI such lists included customers and co-conspirators that sold cellular  
 26 phone unlocking services to the public.

27      39. GHULAM JIWANI caused the lists of IMEIs to be submitted to the AT&T  
 28 insiders so that the AT&T insiders could unlock the cellular phones. GHULAM JIWANI

1 subsequently received reports from the AT&T insiders showing which IMEIs had been  
2 unlocked, and forwarded these to customers and co-conspirators. GHULAM JIWANI  
3 also negotiated and obtained payments from customers of the conspiracy.

4 40. GHULAM JIWANI made bribe payments to insiders at AT&T.  
5 GHULAM JIWANI did so by causing payments to be transmitted by Western Union to  
6 the insiders. GHULAM JIWANI also did so by flying from Pakistan to the United States  
7 and delivering cash payments to the insiders or to persons who received the cash  
8 payments on behalf of the insiders.

9 41. GHULAM JIWANI facilitated, and attended, a meeting between  
10 MUHAMMAD FAHD and one of the AT&T insiders. GHULAM JIWANI did so by  
11 arranging for the insider to travel from the State of Washington to Dubai, United Arab  
12 Emirates, in order to meet with MUHAMMAD FAHD and to receive payment of a bribe  
13 from MUHAMMAD FAHD.

14 All in violation of Title 18, United States Code, Section 1349.

15  
16 **COUNT 2**  
17 **(Conspiracy to Violate the Travel Act and  
the Computer Fraud and Abuse Act)**

18 42. The allegations set forth in Count 1 of this Second Superseding Indictment  
19 are re-alleged and incorporated as if fully set forth herein.

20 **I. THE OFFENSE**

21 43. Beginning at a date uncertain, but no later than April 2013, and continuing  
22 through in or about September 2017, at Bothell, within the Western District of  
23 Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM  
24 JIWANI, and others known and unknown to the Grand Jury, did knowingly and  
25 intentionally agree and conspire to:

26 a. use a facility in interstate and foreign commerce, namely the wires,  
27 with the intent to promote, manage, establish, carry on and facilitate the promotion,  
28

1 management, establishment and carrying on of an unlawful activity, that is, Commercial  
2 Bribery, in violation of the Revised Code of Washington Section 9A.68.060, and  
3 thereafter performed and attempted to perform an act to distribute the proceeds of such  
4 unlawful activity, and to promote, manage, establish and carry on, and to facilitate the  
5 promotion, management, establishment and carrying on of, such unlawful activity in  
6 violation of Title 18, United States Code, Section 1952(a)(1) and (3);

7                   b.       knowingly and with intent to defraud, access a protected computer  
8 without authorization and exceed authorized access to a protected computer, and by  
9 means of such conduct further the intended fraud and obtain anything of value exceeding  
10 \$5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections  
11 1030(a)(4) and (c)(3)(A); and

12                   c.       knowingly cause the transmission of a program, information, code,  
13 and command, and as a result of such conduct, intentionally cause damage without  
14 authorization to a protected computer, and the offense caused loss to 1 or more persons  
15 during any 1-year period aggregating at least \$5,000 in value and damage affecting 10 or  
16 more protected computers during a 1-year period, in violation of Title 18, United States  
17 Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

## 18           II.    THE OBJECT OF THE CONSPIRACY

19           44.      The object of the conspiracy is set forth in Paragraph 15 of this Second  
20 Superseding Indictment and is re-alleged and incorporated as if fully set forth herein.  
21 Through their conduct, the conspirators caused damages to AT&T's protected computers,  
22 including impairment to the integrity and availability of data, programs, systems, and  
23 information, and caused losses to AT&T for the costs of responding to the offense,  
24 conducting damage assessments, restoring data, programs, systems and information and  
25 lost revenue during any 1-year period in excess of \$5,000.00.

1           **III. THE MANNER AND MEANS OF THE CONSPIRACY**

2           45. The manner and means of the conspiracy are set forth in Paragraphs 16  
3 through 41 of this Second Superseding Indictment and are re-alleged and incorporated as  
4 if fully set forth herein.

5           **IV. OVERT ACTS**

6           46. In furtherance of the conspiracy, and to achieve the objects thereof,  
7 defendants MUHAMMAD FAHD, GHULAM JIWANI and others known and unknown  
8 to the Grand Jury, did commit and cause to be committed, the following overt acts, at  
9 Bothell, within the Western District of Washington and elsewhere:

10           a. On or about April 11, 2013, MUHAMMAD FAHD opened a Yahoo  
11 account with the email address unlockoutlet@ymail.com;

12           b. In or about April 2013, MUHAMMAD FAHD provided two AT&T  
13 insiders (CC-2 and CC-3) who were employed at AT&T in Bothell, Washington, with  
14 malware;

15           c. In or about April 2013, each of those AT&T insiders (CC2 and  
16 CC-3) installed the malware on AT&T's internal protected network;

17           d. On or about April 15, 2013, a co-conspirator wired bribe payments  
18 in the amount of \$11,000.00 to each of the two AT&Ts insiders (CC-2 and CC-3) from  
19 California to Marysville, Washington;

20           e. On or about November 12, 2014, MUHAMMAD FAHD sent a  
21 WhatsApp message to GHULAM JIWANI instructing him to send a \$4,000 bribe by  
22 Western Union to one AT&T insider (CC-2) and a \$1,000 bribe by Western Union to  
23 another AT&T insider (CC-5);

24           f. On or about November 25, 2014, MUHAMMAD FAHD sent a  
25 router to an AT&T insider (CC-2) via Federal Express from Dubai, United Arab  
26 Emirates, to Lynnwood, Washington;

g. In or about November 2014, the AT&T insider (CC-2) provided a router configured to provide unauthorized access to AT&T's internal protected network to another AT&T insider (CC-5) to install on AT&T's network;

h. On or about August 9, 2015, MUHAMMAD FAHD and GHULAM JIWANI traveled to Dubai, United Arab Emirates, from Karachi, Pakistan, to meet an AT&T insider (CC-2) and to deliver a bribe payment to him;

i. On or about February 26, 2015, GHULAM JIWANI traveled to Houston, Texas, to deliver a bribe for an AT&T insider (CC-5).

All in violation of Title 18, United States Code, Section 371.

**COUNTS 3-6**  
**(Wire Fraud)**

47. The allegations set forth in Counts 1 and 2 of this Second Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

## I. THE SCHEME

48. Beginning at a date uncertain, but no later than April 2012, and continuing through in or about September 2017, at Bothell, within the Western District of Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM JIWANI, and others known and unknown to the Grand Jury, devised and intended to devise a scheme to defraud AT&T Mobility LLC, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.

## II. THE MANNER AND MEANS OF THE SCHEME

49. The manner and means of the scheme are set forth in Paragraphs 16 through 41 of this Second Superseding Indictment and are re-alleged and incorporated as if fully set forth herein.

1                   **III. EXECUTION OF THE SCHEME**

2               50. On or about the dates set forth below, at Bothell, within the Western  
 3 District of Washington, and elsewhere, MUHAMMAD FAHD, GHULAM JIWANI, and  
 4 others known and unknown to the Grand Jury, having devised a scheme and artifice to  
 5 defraud, and to obtain money and property by means of materially false and fraudulent  
 6 pretenses, representations, and promises, did knowingly transmit and cause to be  
 7 transmitted writings, signs, signals, pictures, and sounds, for the purpose of executing  
 8 such scheme, by means of wire communication in interstate and foreign commerce,  
 9 including the following transmissions, with each such transmission constituting a  
 10 separate count of this Second Superseding Indictment.

Count	Date(s)	Defendant(s) Charged	Wire Communication
3	April 6, 2013	MUHAMMAD FAHD GHULAM JIWANI	Email from an AT&T insider (CC-3) at Bothell, Washington, to MUHAMMAD FAHD, outside the State of Washington, which then was forwarded by MUHAMMAD FAHD to GHULAM JIWANI, reporting on the status of cellular telephone unlocks for a list of cellular telephone IMEIs
4	April 19, 2013	MUHAMMAD FAHD	Email from MUHAMMAD FAHD from outside the State of Washington, to an AT&T insider (CC-2) at Bothell, Washington, with attached malware and with instructions for installing the malware on AT&T's computer system
5	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Western Union transfer of \$4,052 from outside the State of Washington to Lynnwood, Washington, to pay a bribe to an AT&T insider (CC-2)

Count	Date(s)	Defendant(s) Charged	Wire Communication
6	January 8, 2015	MUHAMMAD FAHD	E-mail from an AT&T insider (CC-5) at Bothell, Washington, to MUHAMMAD FAHD, outside the State of Washington, containing photographs of the AT&T insider's work computer screen

7 All in violation of Title 18, United States Code, Sections 1343 and 2.  
 8  
 9

10 **COUNT 7**  
 11 **(Accessing a Protected Computer in Furtherance of Fraud)**

12 51. The allegations set forth in Counts 1 through 6 of this Second Superseding  
 13 Indictment are re-alleged and incorporated as if fully set forth herein.

14 52. Beginning at a date uncertain, but no later than in or about April 2013, and  
 15 continuing until in or around October 2013, at Bothell, within the Western District of  
 16 Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others known  
 17 and unknown to the Grand Jury, knowingly and with intent to defraud accessed protected  
 18 computers without authorization and exceeded authorized access and by means of such  
 19 conduct furthered the intended fraud and obtained something of value, specifically, the  
 20 defendant and others downloaded and installed malware onto AT&T Mobility LLC's  
 21 protected computers and executed the malware programs designed to facilitate fraudulent  
 22 and unauthorized unlocking transactions on AT&T Mobility LLC's wireless network and  
 23 by means of such conduct furthered the intended fraud and obtained things of value  
 24 exceeding \$5,000.00 in any 1-year period.

25 All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A)  
 26 and 2.  
 27  
 28

**COUNT 8**

53. The allegations set forth in Counts 1 through 7 of this Second Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

5 54. Beginning at a date uncertain, but no later than in or about April 2013, and  
6 continuing until in or around October 2013, at Bothell, within the Western District of  
7 Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others known  
8 and unknown to the Grand Jury, knowingly caused the transmission of a program,  
9 information, code, and command, specifically malicious code that was downloaded and  
10 installed on AT&T Mobility LLC's protected computers without AT&T Mobility LLC's  
11 knowledge or consent, and as a result of such conduct, intentionally caused damage  
12 without authorization to protected computers, which damage caused losses to 1 or more  
13 persons during any 1-year period of at least \$5,000.00 and affected 10 or more protected  
14 computers during a 1 year period.

15 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and  
16 (c)(4)(B)(i) and 2.

**COUNT 9**

55. The allegations set forth in Counts 1 through 8 of this Second Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

22       56. Beginning at a date uncertain, but no later than in or about November 2014,  
23 and continuing until in or around September 2017, at Bothell, within the Western District  
24 of Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others  
25 known and unknown to the Grand Jury, knowingly and with intent to defraud accessed  
26 protected computers without authorization and exceeded authorized access and by means  
27 of such conduct furthered the intended fraud and obtained something of value,  
28 specifically, the defendant and others installed malware and unauthorized hardware onto

1 AT&T Mobility LLC's protected computers designed to facilitate fraudulent and  
2 unauthorized unlocking transactions on AT&T Mobility LLC's wireless network and by  
3 means of such conduct furthered the intended fraud and obtained things of value  
4 exceeding \$5,000.00 in any 1-year period.

5 All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A)  
6 and 2.

7

8

9 **COUNT 10**  
**(Intentional Damage to a Protected Computer)**

10 57. The allegations set forth in Counts 1 through 9 of this Second Superseding  
11 Indictment are re-alleged and incorporated as if fully set forth herein.

12 58. Beginning at a date uncertain, but no later than in or around November  
13 2014, and continuing until in or around September 2017, at Bothell, within the Western  
14 District of Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and  
15 others known and unknown to the Grand Jury, knowingly caused the transmission of a  
16 program, information, code, and command, through malware and unauthorized hardware  
17 that was installed on AT&T Mobility LLC's protected computers without AT&T  
18 Mobility LLC's knowledge or consent, and as a result of such conduct, intentionally  
19 caused damage without authorization to protected computers, which damage caused  
20 losses to 1 or more persons during any 1-year period of at least \$5,000.00 and affected 10  
21 or more protected computers during a 1 year period.

22 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and  
23 (c)(4)(B)(i) and 2.

## COUNTS 11-14 (Travel Act)

59. The allegations set forth in Counts 1 through 10 of this Second Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

60. On or about the dates below, at Bothell, within the Western District of Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM JIWANI, and others known and unknown to the Grand Jury, used a facility in interstate and foreign commerce with the intent to distribute the proceeds, and to promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on, of an unlawful activity, that is: Commercial Bribery in violation of Revised Code of Washington Section 9A.68.060, and thereafter performed and attempted to perform an act to distribute the proceeds, and to promote, manage, establish and carry on and facilitate the promotion, management, establishment and carrying on, of such unlawful activity.

Count	Date(s)	Defendant(s) Charged	Act Performed
11	April 15, 2013	MUHAMMAD FAHD	Payment of \$11,000, by wire transfer, from an account outside the State of Washington to an account at Chase Bank within the State of Washington to pay a bribe to an AT&T insider (CC-3)
12	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Payment of \$4,052 by Western Union, from outside the State of Washington, to an AT&T insider (CC-2) in Lynnwood, Washington, to pay a bribe to that insider
13	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Payment of \$948 by Western Union, from outside the State of Washington, to an AT&T insider (CC-5), in Everett, Washington, to pay a bribe to that insider

Count	Date(s)	Defendant(s) Charged	Act Performed
14	August 10, 2015	MUHAMMAD FAHD GHULAM JIWANI	Purchase of ticket for flight by an AT&T insider (CC-2), and subsequent flight by that insider, by commercial airline from SeaTac, Washington, to Dubai, United Arab Emirates, to meet MUHAMMAD FAHD and GHULAM JIWANI

All in violation of Title 18, United States Code, Sections 1952(a)(1) and (3), and 2.

### FORFEITURE ALLEGATIONS

61. The allegations contained in Counts 1 through 14 of this Second Superseding Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i).

62. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Section 1349, as set forth in Count 1, of a violation of Title 18 United States Code, Section 1343, as set forth in Counts 3 through 6, the defendants shall forfeit to the United States of America, any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

63. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), in violation of Title 18, United States Code,

1 Section 371, as set forth in Count 2, the defendants shall forfeit to the United States of  
 2 America any property, real or personal, which constitutes or is derived from proceeds  
 3 traceable to the charged offense, and any personal property that was used or intended to  
 4 be used to commit or to facilitate the commission of such offense. The property to be  
 5 forfeited includes, but is not limited to, the following: a sum of money representing the  
 6 amount of proceeds the defendant obtained as a result of the charged offense.

7 64. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title  
 8 18, United States Code, Section 1030(i) , upon conviction of a violation of Title 18,  
 9 United States Code, Sections 1030(a)(4) and (c)(3)(A), as set forth in Counts 7 and 9, the  
 10 defendant shall forfeit to the United States of America any property, real or personal,  
 11 which constitutes or is derived from proceeds traceable to the charged offense, and any  
 12 personal property that was used or intended to be used to commit or to facilitate the  
 13 commission of such offense. The property to be forfeited includes, but is not limited to,  
 14 the following: a sum of money representing the amount of proceeds the defendant  
 15 obtained as a result of the charged offense.

16 65. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title  
 17 18, United States Code, Section 1030(i) , upon conviction of a violation of Title 18,  
 18 United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), as set forth in Counts 8 and  
 19 10, the defendant shall forfeit to the United States of America any property, real or  
 20 personal, which constitutes or is derived from proceeds traceable to the charged offense.  
 21 The property to be forfeited includes, but is not limited to, the following: a sum of money  
 22 representing the amount of proceeds the defendant obtained as a result of the charged  
 23 offense.

24 66. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28,  
 25 United States Code, Section 2461(c), upon conviction of a Travel Act violation, in  
 26 violation of Title 18, United States Code, Section 1952(a)(1) and (3), as set forth in  
 27 Counts 11 through 14, the defendants shall forfeit to the United States of America any  
 28 property, real or personal, which constitutes or is derived from proceeds traceable to the

1 charged offense. The property to be forfeited includes, but is not limited to, the  
2 following: a sum of money representing the amount of proceeds the defendant obtained  
3 as a result of the charged offense.

4 67. If any of the property described above, as a result of any act or omission  
5 of the defendants:

6 a. cannot be located upon the exercise of due diligence;  
7 b. has been transferred or sold to, or deposited with, a third party;  
8 c. has been placed beyond the jurisdiction of the court;  
9 d. has been substantially diminished in value; or  
10 e. has been commingled with other property which cannot be divided  
11 without difficulty, the United States of America shall be entitled to

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

1 forfeiture of substitute property pursuant to Title 21, United States  
2 Code, Section 853(p), as incorporated by Title 28, United States  
3 Code, Section 2461(c).  
4

5 A TRUE BILL:  
6

7 DATED: *1 March 2018*  
8

9 (Signature of Foreperson redacted pursuant  
10 to the policy of the Judicial Conference)  
11

12 FOREPERSON  
13

14 *Leslie S. Samuels*  
15 ANNETTE L. HAYES  
16 United States Attorney

17 *Andrew C. Friedman*  
18 ANDREW C. FRIEDMAN  
19 Assistant United States Attorney

20 *Francis Franze-Nakamura*  
21 FRANCIS FRANZE-NAKAMURA  
22 Assistant United States Attorney

23 *Andrew S. Pak*  
24 ANDREW S. PAK  
25 Trial Attorney  
26 Computer Crimes and Intellectual Property Section